bananaz

The Agentic Layer for Mechanical Engineers

bananaz Security & Trust Overview

Secure-by-design platform for engineering teams
Resilient to protect your product data

Overview

bananaz AI agents understand CAD models, drawings, and BOMs. They automate design reviews, detect and document changes, enforce engineering standards, and deliver DFM insights to supercharge your CAD and PDM tools and accelerate design-to-manufacturing, built with a security-first mindset.

The platform built on Amazon Web Services (AWS) and architected with security as a first-class feature, not an afterthought. Our platform runs in logically isolated AWS VPCs with network security groups, web application firewalls, and strict separation between environments, so customer workloads stay isolated.

bananaz maintains a SOC 2 Type II report for the Security trust category, with an independent auditor attesting that our controls are suitably designed and operated effectively.

Prospects and customers can access our latest security documentation, and key policies through the bananaz Trust & Security Portal at trust.bananaz.ai, which centralizes product security, data protection, infrastructure, and policy information.

Reducing your risk with bananaz

Because security is built into the platform, bananaz helps you reduce the operational and compliance risk of managing complex CAD and PDM workflows yourself. Centralized, access-controlled collaboration means fewer unmanaged file shares and email attachments, while comprehensive logging and audit trails strengthen your ability to demonstrate control over design changes and approvals.

aws

Secure user access and collaboration

All access to the bananaz platform and customer data is authenticated and authorized. End users access bananaz through a web browser over HTTPS. Authentication can be integrated with your existing identity provider using SSO. Access to workspaces, projects, and design data is governed by permissions-based access controls, ensuring users only see the drawings and change information they are authorized to work on. Sessions are protected with multi-factor authentication and strong password policies, and all sign-ins, approvals, comments, and data access actions are logged and monitored, giving you a clear audit trail of who accessed what and when.

Application security

All of our applications components are subject to security assessments for major releases, and at least annual third-party penetration testing, with high and critical findings remediated promptly under our Application Security Policy and SOC 2–tested controls. Production access for developers is limited and audited.

Secure coding practices

the bananaz Platform utilizes secure coding practices based on best practices prescribed by the Open Web Application Security Project (OWASP). All the bananaz Platform, Software Engineers are required to complete yearly training and testing on secure coding practices. the bananaz Platform leverages tools to assess the security of the code and employs a secure coding audit as part of code reviews.

Monitoring, logging, and incident response

All activity on the bananaz platform is logged and monitored, including authentication, administrative actions, and sensitive operations. Logs from AWS (CloudTrail, GuardDuty, WAF, and related services) and application components are retained for up to one year and used to detect anomalous or potentially malicious behavior. Our Incident Management Policy defines a formal Security Response Team, clear escalation paths, evidence preservation, and root-cause analysis for security events and personal data breaches, including customer and regulatory notifications where required. Customers can report potential incidents at any time via security@bananaz.ai .

Data security

All customer data is encrypted in transit using TLS 1.2 or higher and at rest using strong AES-256 encryption, both at the application and AWS storage layers. Access to production systems, identity management, source control, and backup administration is restricted to authorized personnel and always protected with multi-factor authentication and strong password standards. We enforce role-based access control with unique user IDs, least-privilege permissions, and quarterly access reviews by management.

Find out more at:

trust.bananaz.ai